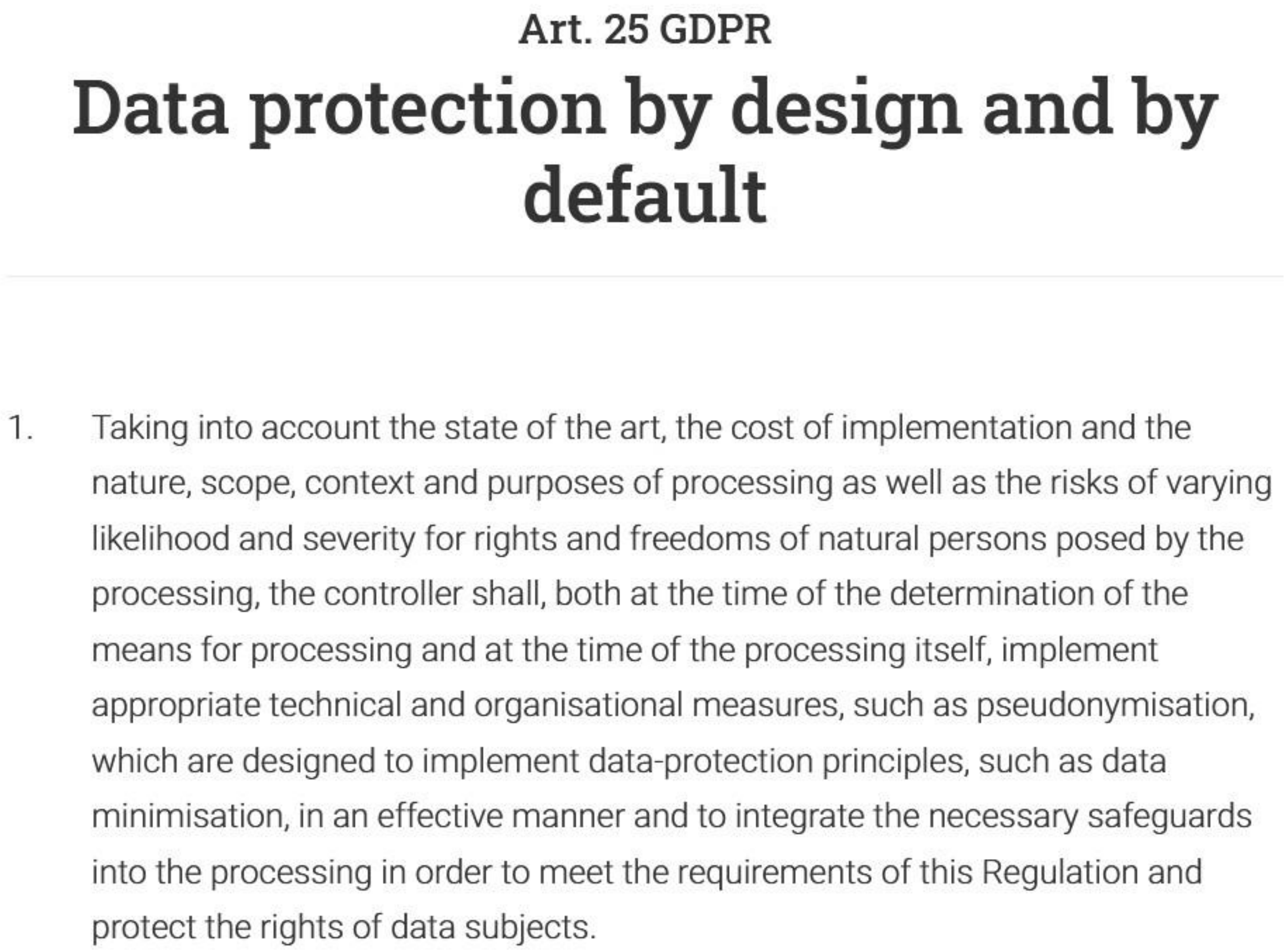
Lecture 14:
Privacy Engineering

CMSC 25900 / DATA 25900

Spring 2021

The University of Chicago



Art. 25 GDPR

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

https://gdpr-info.eu/art-25-gdpr/

Privacy By Design (PbD)
& Privacy Engineering

Potential Goals of Privacy Engineering

- Compliance with laws
    - GDPR, CCPA, etc.
- Compliance with reasonable consumer expectations and making accurate public statements
    - See, e.g., FTC’s mandates
- Engender trust and goodwill among your users
    - “Competing” based on privacy-protectiveness
- Protecting privacy as a societal value / “it’s the right thing”

Mechanisms

- Not collecting data
  - Selective collection, immediate de-identification
- Not retaining data
- Thoughtful applications of cryptographic tools
- Thoughtful architectures for computer systems
  - Access control, data storage
- Public statements and user communication (e.g., in UIs)
- Appropriate socio-technical processes, audits, and reviews

Privacy Impact Assessments (PIAs)

- "A PIA is an analysis of how personally identifiable information is collected, used, disseminated, and maintained. It examines how the Department has incorporated privacy concerns throughout its development, design, and deployment of a technology, program, or rulemaking. "Personally identifiable information" is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual"

https://www.dhs.gov/sites/default/files/publications/privacy_pia_guidance_june2010_0.pdf

Privacy Impact Assessments (PIAs)

- “The purpose of a PIA is to demonstrate that program managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or program. This involves making certain that privacy protections are built into the system from the initiation of development, not after the fact when they can be far more costly or could affect the viability of the project. The PIA process requires that candid and forthcoming communications occur between the program manager, system owner, the component’s Privacy Officer, and the Privacy Office to ensure appropriate and timely handling of privacy concerns. Addressing privacy issues publicly through a PIA builds citizen trust...”

https://www.dhs.gov/sites/default/files/publications/privacy_pia_guidance_june2010_0.pdf

Case Studies

In-store Tracking

- **Setting:** BlaseMart wants to track customers as they move through the store to:
  - Understand which areas of the store are most popular
  - Optimize the relative location of different displays by understanding which sections are highly correlated among consumers' visits
  - Provide targeted discounts to specific consumers about specific products

Maps App

- **Setting:** Blaze (like Waze, but better) wants to provide a privacy-protective alternative to Google Maps
  - Real-time traffic info
  - Accident/closure reporting
  - Convenient history-based recommendations for users

Messaging App

- **Setting:** Signal wants to provide a “more secure” alternative to Facebook Messenger

Browser

- **Setting:** The Blazefox web browser wants to determine what malware websites its users have visited
  - Caveat: The malware sites are only identified after the fact

Voice Assistant

- **Setting:** Amazon wants to improve the speech recognition on the Amazon Echo